KA / BG-GPO / 2515 / WPP-47 / 2009-2011



ಕರ್ನಾಟಕ ರಾಜ್ಯಪತ್ರ

ಅಧಿಕೃತವಾಗಿ ಪ್ರಕಟಿಸಲಾದುದು

ಸಂಪುಟ ೧೪೪	ಬೆಂಗಳೂರು, ಗುರುವಾರ, ಮೇ ೭, ೨೦೦೯ (ವೈಶಾಖ ೧೭, ಶಕ ವರ್ಷ ೧೯೩೧)	ಸಂಚಿಕೆ ೧೯

ಭಾಗ – ೪

ಕೇಂದ್ರದ ವಿಧೇಯಕಗಳು ಮತ್ತು ಅವುಗಳ ಮೇಲೆ ಪರಿಶೀಲನಾ ಸಮಿತಿಯ ವರದಿಗಳು, ಕೇಂದ್ರದ ಅಧಿನಿಯಮಗಳು ಮತ್ತು ಅಧ್ಯಾದೇಶಗಳು, ಕೇಂದ್ರ ಸರ್ಕಾರದವರು ಹೊರಡಿಸಿದ ಸಾಮಾನ್ಯ ಶಾಸನಬದ್ಧ ನಿಯಮಗಳು ಮತ್ತು ಶಾಸನಬದ್ಧ ಆದೇಶಗಳು ಮತ್ತು ರಾಷ್ಟ್ರಪತಿಯವರಿಂದ ರಚಿತವಾಗಿ ರಾಜ್ಯ ಸರ್ಕಾರದವರಿಂದ ಪುನಃ ಪ್ರಕಟವಾದ ಆದೇಶಗಳು.

ಸಂಸದೀಯ ವ್ಯವಹಾರಗಳು ಮತ್ತು ಶಾಸನ ರಚನೆ ಸಚಿವಾಲಯ

ಅಧಿಸೂಚನೆ

ಸಂಖ್ಯೆ: ಸಂವ್ಯಶಾಇ 25 ಕೇಶಾಪ್ರ 2009, ಬೆಂಗಳೂರು, ದಿನಾಂಕ: 2ನೇ ಮಾರ್ಚ್ 2009

2009ನೇ ಸಾಲಿನ ಫೆಬ್ರವರಿ 5ನೇ ದಿನಾಂಕದ ಭಾರತ ಸರ್ಕಾರದ ಗೆಜೆಟಿನ ವಿಶೇಷ ಸಂಚಿಕೆಯ ಭಾಗ–II ಸೆಕ್ಷನ್ 1 ರಲ್ಲಿ ಪ್ರಕಟವಾದ ಈ ಕೆಳಕಂಡ The Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009) ಅನ್ನು ಸಾರ್ವಜನಿಕರ ಮಾಹಿತಿಗಾಗಿ ಕರ್ನಾಟಕ ರಾಜ್ಯ ಪತ್ರದಲ್ಲಿ ಮರು ಪ್ರಕಟಿಸಲಾಗಿದೆ.

MINISTRY OF LAW AND JUSTICE

(Legislative Department)

New Delhi, the 5th February, 2009 / Magha 16, 1930 (Saka)

The following Act of Parliament received the assent of the President on the 5th February, 2009, and is hereby published for general information:

THE INFORMATION TECHNOLOGY (AMENDMENT) ACT , 2008

No. 10 OF 2009

[5th February, 2009.]

An Act further to amend the Information Technology Act, 2000.

BE it enacted by Parliament in the Fifty-ninth Year of the Republic of India as follows:

PART -I

PRELIMINARY

I. Short title and commencement : (I) This Act may be called the Information Technology (Amendment) Act, 2008.

(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint:

Provided that different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

PART II

AMENDMENTS TO THE INFORMATION TECHNOLOGY ACT, 2000

2. Substitution of words "digital signature" by words "electronic signature" : In the Information Technology Act, 2000 (hereinafter in this Part referred to as the 2 principal Act), for the words "digital signature" occurring in the Chapter, section, sub-section and clause referred to in the Table below, the words "electronic signature" shall be substituted.

TABLE

S.No.	Chapter/section/sub-section/clause
(1)	clauses (d), (g) (h) and (zg) of section 2;
(2)	section 5 and its marginal heading;
(3)	marginal heading of section 6;
(4)	clauses (a), (b), (c) and (e) of section 10 and its marginal heading;
(5)	heading of Chapter V;
(6)	clauses (f) and (g) of section 18;
(7)	sub-section (2) of section 19;
(8)	sub-sections (1) and (2) of section 21 and its marginal heading;
(9)	sub-section (3) of section 25;
(10)	clause (c) of section 30;
(11)	clauses (a) and (d) of sub-section (1) and sub-section (2) of section 34;
(12)	heading of Chapter VII;
(13)	section 35 and its marginal heading;
(14)	section 64;
(15)	section 71;
(16)	sub -section (1) of section 73 and its marginal heading;
(17)	section 74, and
(18)	clauses (d), (n) and (o) of sub-section (2) of section 87. —

3. Amendment of section 1:- In section 1 of the principal Act, for sub-section (4), the following sub-sections shall be substituted, namely:

"(4) Nothing in this Act shall apply to documents or transactions specified in the First Schedule:

Provided that the Central Government may, by notification in the Official Gazette, amend the First Schedule by way of addition or deletion of entries thereto.

(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.".

4. Amendment of section 2:- In section 2 of the principal Act,-

(A) after clause (h), the following clause shall be inserted, namely:

'(ha) "communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;';

(B) for clause (j) the following clause shall be substituted, namely:

'(j) "computer network" means the inter—connection of one or more computers or computer Systems or communication device through—

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the inter-connection is continuously maintained;';

(C) in clause (n), the word "Regulations" shall be omitted;

(D) after clause (n), the following clauses shall be inserted, namely:

'(na) " cyber cafe" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public;

(nb) "cyber security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction;'.

(E) after clause (t), the following clauses shall be inserted, namely:-

(ta) "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;

(tb) "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate;';

(F) after clause (u), the following clause shall be inserted, namely:-

'(ua) "Indian Computer Emergency Response Team" means an agency established under sub-section (1) of section 70B;';

(G) in clause (v), for the words "data, text", the words "data, message, text" shall be substituted;

(H) for clause (w), the following clause shall be substituted, namely:-

(w) "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;'.

5. Amendment of heading of chapter II: In Chapter II of the principal Act, for the heading, the heading "DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE" shall be substituted.

6. Insertion of new section 3A: After section 3 of the principal Act, the following section shall be inserted, namely:—

"3A. Electronic signature : (1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate may electronic record by such electronic signature or electronic authentication technique which-

(a) is considered reliable; and

(b) may be specified in the Second Schedule.

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if—

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature detectable; and

(e) it fulfils such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule:

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.

7. Insertion of new section 6A : After section 6 of the principal Act, the following section shall be inserted, namely:

6A. Delivery of services by service provider : (1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorise, by order, any service provider to set up, maintain and upgrade the computerised facilities and perform such other services as it may specify by notification in the Official Gazette.

Explanation.- For the purposes of this section, service provider so authorised includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

(2) The appropriate Government may also authorise any service provider authorised under sub-section (1) to collect, retain and appropriate such service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(3) Subject to the provisions of sub-section (2), the appropriate Government may authorise the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

(4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.'.

8. Insertion of new section 7A : After section 7 of the principal Act, the following section shall be inserted, namely:—

"7A. Audit of documents etc., maintained in electronic form : Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of' documents, records or information processed and maintained in the electronic form".

9. Insertion of new section 10A : After section 10 of the principal Act, the following section shall be inserted namely:—

"10A. Validity of contracts formed through electronic means : Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose."

10. Amendment of section 12 : In section 12 of the principal Act, in sub-section (1), for the words "agreed with the addressee", the word "stipulated" shall be substituted.

11. Substitution of new sections for sections 15 and 16 : For sections 15 and 16 of the principal Act, the following sections shall be substituted, namely :-

"15. Secure electronic signature : An electronic signature shall be deemed to be a secure electronic signature if-

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation.- In case of digital signature, the "signature creation data" means the private key of the subscriber.

16. Security procedures and practices : The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices :

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate "

12. Amendment of section 17 : In section 17 of the principal Act,,-

(a) in sub-section (1), for the words "and Assistant Controllers", the words", Assistant Controllers, other officers and employees" shall be substituted". and

(b) in sub-section (4), for the words "and Assistant Controllers", the words, "Assistant Controllers, other officers and employees" shall be substituted."

13. Omission of section 26 : Section 20 of the principal Act shall be omitted

14. Amendment of section 29 : In section 29 of the principal Act, in sub-section (1) for the words "any contravention of the provisions of this Act, rules or regulations made thereunder", the words "any contravention of the provisions of this Chapter" shall be substituted.

15. Amendment of section 30 : In section 30 of the principal Act,

(i) in clause (c), after the word "assured", the word "and" shall be omitted;

(ii) after clause (c) the following clauses shall be inserted, namely :-

"(ca) be the repository of the electronic Signature Certificates issued under this Act;

(cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and."

16. amendment of section 34 : In section 34 of the principal Act, in sub-section (1) in clause (a), the words "which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital signature Certificate" shall be omitted.

17. Amendment of section 35 : In section 35 of the principal Act, in sub – section (4) –

(a) the first proviso shall be omitted

(b) in the second proviso, for the words "Provided further" the word "Provided" shall be substituted.

18. Amendment of section 36 : In section 36 of the principal Act, after clause (c), the following clauses shall be inserted, namely :-

"(ca) the subscriber holds a private key which is capable of creating a digital signature ;

(cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key hold by the subscriber ;.

19. Insertion of new section 40A: After section 40 of the principal Act, the following section shall be inserted, namely:—

Duties of subscriber of Electronic Signature Certificate : " 40 A. In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.".

20. Amendment of heading of Chapter IX : In Chapter IX of the principal Act, in the heading, for the words "PENALTIES AND ADJUDICATION", the words "PENALTIES, COMPENSATION AND ADJUDICATION" shall be substituted

21. Amendment of section 43 : In section 43 of the principal Act,—

(a) in the marginal heading, for the word "Penalty" the words "Penalty and Compensation" shall be substituted;

(b) in clause (a), after the words "computer network", the words "or computer resource" shall be inserted;

(c) after clause (h), the following clauses shall be inserted, namely:—

"(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;";

(d) for the portion begining with the words "he shall be liable to pay damages" and ending with the words "persons so affected" the following shall be substituted, namely:—

"he shall be liable to pay damages by way of compensation to the person so affected"

(e) in the Explanation, after clause (iv), the following clause shall be inserted, namely:—

'(v) "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.".

22. Insertion of new section 43 A : After section 43 of the principal Act, the following section shall be inserted, namely:—

"43A. Compensation for failure to protect data: Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation - For the purposes of this section,—

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

23. Amendment of section 46 : In section 46 of the principal Act,

(a) in sub-section (1), for the words "direction or order made thereunder", the words "direction or order made thereunder which renders him liable to pay penalty or compensation," shall be substituted;

(b) after sub-section (1), the following sub-section shall be inserted, namely:—

"(1A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore:

Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crore shall vest with the competent court.";

(c) in sub-section (5), after clause (b), the following clause shall be inserted, namely:—

"(c) shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908 (5 of 1908);

24. Amendment of heading of chapter X : In Chapter X of the principal Act, in the heading, the word "REGULATIONS" shall be omitted.

25. Amendment of section 48 : In section 48 of the principal Act, in sub-section (1), the word "Regulations" shall be omitted.

26. Substitution of new sections for sections 49 to 52 : For sections 49 to 52 of the principal Act, the following sections shall be substituted, namely:—

"49. Composition of Cyber appellate Tribunal : (1) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint:

Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the Information Technology (Amendment) Act, 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008.

(2) The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.

(3) Subject to the provisions of this Act—

(a) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof,

(b) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two Members of such Tribunal as the Chairperson may deem fit;

(c) the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify;

(d) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.

(4) Notwithstanding anything contained in sub-section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench.

(5) If at any stage of the hearing of any case or matter it appears to the Chairperson or a Member of the Cyber Appellate tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit.

50. Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal: (1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court.

(2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (3), shall be appointed by the Central Government from amongst persons, having special knowledge of, and professional experience in, information technology, telecommunication, industry, management or consumer affairs:

Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than one year or Joint Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than seven years.

(3) The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian legal Service and has held the post of Additional Secretary for a period of not less than one year or Grade I post of that Service for a period of not less than five years.

51. Term of office, conditions of service, etc., of Chairperson and Members : (1) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

(2) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member,

(3) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal as the case may be, shall have to retire from service before joining as such Chairperson or Member.

52. Salary, allowances and other terms and conditions of service of Chirperson and Members: The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of the Cyber Appellate Tribunal shall be such as may be prescribed.

52A. Powers of superintendence, direction, etc : The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.

52B. Distribution of business among Benches : Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench.

52C. Power of Chairperson to transfer cases : On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or suo motu without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench.

52D. Decision by majority : If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.".

27. Amendment of section 53 : In section 53 of the principal Act, for the words "Presiding Officer", the words "Chairperson or Member, as the case may be," shall be substituted.

28. Amendment of section 54 : In section 54 of the principal Act, for the words "Presiding Officer" wherever they occur, the words "Chairperson or the Member" shall be substituted.

29. Amendment of section 55 : In section 55 of the principal Act, for the words "Presiding Officer", the words "Chairperson or the Member" shall be substituted.

30. Amendment of section 56 : In section 56 of the principal Act, for the words presiding Officer" the word "Chairperson" shall be substituted.

31. Amendment of section 64 : In section 64 of the principal Act,—

(i) for the words "penalty imposed", the words "penalty imposed or compensation awarded" shall be substituted;

(ii) in the marginal heading, for the word "penalty", the words "penalty or compensation" shall be substituted.

32. Substitution of new sections for sections 66 and 67 : For sections 66 and 67 of the principal Act, the following sections shall be substituted, namely:—

"66. Computer related offences: If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation. - For the purposes of this section,

(a) the word "dishonestly" shall have the meaning assigned to it in section 24 (45 of 1860)of the Indian Penal Code;

(b) the word "fraudulently" shall have the meaning assigned to it in section 25 (45 of 1860) of the Indian Penal Code.

66A. Punishment for sending offensive messages through communication service, etc : Any person who sends, by means of a computer resource or a communication device,—

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(c) any eletronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.— For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

66B. Punishment for dishonestly receiving stolen computer resource or communication device : Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both

66C. Punishment for identity theft : Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66D. Punishment for cheating by personation by using computer resource : Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

66E. Punishment for violation of privacy : Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation. - For the purposes of this section—

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, public area, buttocks or female breast;

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that—

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured or

(ii) any part of his or her private area would not he visible to the public, regardless of whether that person is in a public or private place

66F. Punishment for cyber terrorism : (1) Whoever,-

(A)with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant.

And by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B)knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

67. Punishment for publishing or transmitting obscene material in electronic form : Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees:

67A. Punishment for publishing or transmitting of material containing sexually explicitact, etc, in electronic form : Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

67B. Punishment for publishing of transmitting of material depicting children in sexually explicit act, etc, in electronic form : Whoever -,

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online; or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or

subsequent conviction with imprisonment of either discription for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form—

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is in the interest of science, Literature, art or learning of other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes.

Explanation.— For the purposes of this section, "children" means a person who has not completed the age of 18 years.

67C. Preservation and retention of information by intermediaries : (1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.'.

33. Amendment of section 68 : In section 68 of the principal Act, for sub-section (2), the following sub-section shall be substituted, namely:—

"(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both,"

34.Substitution of new sections for section 69 : For section 69 of the principal Act, the following sections shall be substituted namely:

'69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource : (1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of india, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any Computer resource.

(2) The Procedure and safeguards subject to which such interception of monitoring of decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of time computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section *(3)* shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

69A. Power to issue directions for blocking for public access of any information through any computer resource : *(1)* Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section *(2),* for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource,

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section *(1)* shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security : (1) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The intermediary or any person in-charge or the computer resource shall, when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which any extend to three years and shall also be liable to fine.

Explanation.- For the purposes of this section,—

(i) "computer contaminant" shall have the meaning assigned to it in section 43;

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date size, duration or type of underlying service and any other information.

35. Amendment of section 70 : In section 70 of the principal Act,—

(a) for sub-section (1), the following sub-section shall be substituted, namely:-

'(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation.- For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.';

(b) after sub-section (3), the following sub-section shall be inserted, namely:—

"(4) The Central Government shall prescribe the information security practices and procedures for such protected system.".

36. Insertion of new sections 70A and 70 B : After section 70 of the principal Act, the following sections shall be inserted, namely:—

70A. National nodal agency : (1) The Central Government may, by notification published in the Official Gazette, designate any organisation of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

(2) The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

(3) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

70B. Indian Computer Emergency Response Team to serve as national agency for incident response : (1) The Central Government shall, by notification in the Official Gazette, appoint as agency of the Government to be called the Indian Computer Emergency Response Team

(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director - General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.

(4) the Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security.

(a) collection, analysis and dissemination of information on cyber incidents;

(b) forecast and alerts of cyber security incidents;

(c) emergency measures for handling cyber security incidents;

(d) coordination of cyber incidents response activities;

(e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, preventation, response and reporting of cyber incidents;

(f) such other functions relating to cyber security as may be prescribed.

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for Information and give direction to the service providers intermediaries data centres, body corporate and any other person

(7) Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1)"

37. Insertion of new section 72A : After section 72 of the principal Act, the following section shall be inserted, namely:

"72A. Punishment for disclosure of information in breach of lawful contract : Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.".

38. Substitution of new sections for section 77 : For section 77 of the principal Act, the following sections shall be substituted, namely:—

"77. Compensation, penalties or confiscation not to interfere with other punishment : No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

77A. Compounding of offences : A court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided, under this Act:

Provided that the court shall not compound such offence where the accused is, by reason of his previous Conviction, liable to either enhanced punishment or to a punishment of a different kind:

Provided further that the court shall not compound any offence where such offence affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or a woman,

(2) The person accused of an offence under this Act may file an application for compounding in the court in which offence is pending for trial and the provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 (2 of 1974) shall apply.

77B. Offences with three years imprisonment to be bailable : Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974) , the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

39. Amendment of Section 78: In section 78 of the principal Act, for the words "Deputy Superintendent of Police" the word "Inspector" shall be substituted.

40. Substitution of new Chapters for Chapter XII : For Chapter XII of the Principal Act, the following Chapters shall be substituted, namely:

'CHAPTER XII

INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

79. Exemption from liability of intermediary in certain cases : (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted or

(b) the intermediary does not—

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if—

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation. - For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

CHAPTER XIIA

EXAMINER OF ELECTRONIC EVIDENCE

79A. Central Government to notify Exminer of Electronic Evidence : The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation.- For the purposes of this section, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.'.

41. Amendment of section 80 : In section 80 of the principal Act, in sub-section (1), for the words "Deputy Superintendent of Police", the word "Inspector" shall be substituted.

42. Amendment of section 81 : In section 81 of the principal Act, the following proviso shall be inserted at the end, namely:

"Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 (14 of 1957)or the Patents Act, 1970. (39 of 1970)

43. Amendment of section 82 : In section 82 of the principal Act, -

(a) for the marginal heading, the following marginal heading shall be substituted, namely:— "Chairperson, Members, officers and employees to be public servants.";

(b) for the words "Presiding Officer", the words "Chairperson, Members" shall be substituted.

44. Amendment of section 84 : In section 84 of the principal Act, for the words "Presiding Officer" the words "Chairperson, Members" shall be substituted.

45. Insertion of new sections 84A, 84B and 84C : After section 84 of the principal Act, the following sections shall be inserted, namely:—

"84A. Modes of methods for encryption : The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.

84B. Punishment for abetment of offence : Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation.- An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

84C. Punishment for attempt to commit offences : Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.".

46. Amendment of section 87 : In section 87 of the principal Act,—

(A) in sub-section (2),

(i) for clause (a), the following clauses shall be substituted, namely:—

"(a) the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (2) of section 3A;

(aa) the procedure for ascertaining electronic signature or authentication under sub-section (3) of section 3A;

(ab) the manner in which any information or matter may be authenticated by means of electronic signature under section 5;";

(ii) after clause (c), the following clause shall be inserted, namely:-

"(ca) the manner in which the authorised service provider may collect, retain and appropriate service charges under sub-section (2) of section 6A;";

(iii) for clause (e), the following clauses shall be substituted, namely:—

"(e) the manner of storing and affixing electronic signature creation data under section 15;

(ea) the security procedures and practices under section 16;";

(iv) in clause (f), for the words "and Assistant Controllers", the words Assistant Controllers, other officers and employees" shall be substituted;

(v) clause (g) shall be omitted;

(vi) after clause (m) the following clause shall be inserted, namely:

"(ma) the form of application and fee for issue of Electronic Signature Certificate under section 35;";

(vii) after clause (o), the following clauses shall be inserted, namely;.

"(oa) the duties of subscribers under section 40A;

(ob) the reasonable security practices and procedures and sensitive personal data or information under section 43A;";

(viii) in clause (r), for the words "Presiding Officer", the words "Chairperson and Members" shall be substituted;

(ix) in clause (s), for the words "Presiding Officer", the words "Chairperson and Members" shall be substituted;

(x) for clause (w), the following clauses shall be substituted, namely:-

"(w) the powers and functions of the Chairperson of the Cyber Appellate Tribunal under section 52A;

(x) the information, duration, manner and form of such information to be retained and preserved under section 67C;

(y) the procedures and safeguards for interception, monitoring, or decryption under sub-section (2) of section 69;

(z) the procedure and safeguards for blocking for access by the public under sub-section (2) of section 69A;

(za) the procedure and safeguards for monitoring and collecting traffic data or information under sub-section (3) of section 69B;

(zb) the information security practices and procedures for protected system under section 70;

(zc) manner of performing functions and duties of the agency under sub-section (3) of section 70A;

(zd) the officers and employees under sub-section (2) of section 70B;

(ze) salaries and allowances and terms and conditions of service of the Director General and other officers and employees under sub-section (3) of section 70B;

(zf) the manner in which the functions and duties of agency shall he performed under sub-section (5) of section 70B;

(zg) the guidelines to be observed by the intermediaries under sub-section (2) of section 79;

(zh) the modes or methods for encryption under section 84A;";

(B) in sub-section (3),—

(i) for the words, brackets, letter and figures "Every notification made by the Central Government under clause (f) of sub-section (4) of section 1 and every rule made by it", time words "Every notification made by the Central Government under sub-section (1) of section 70A and every rule made by it" shall be substituted;

(ii) the words ''the notification or'' wherever they occur, shall be omitted.

47. Amendment of section 90 : In section 90 of the principal Act, in sub-section (2), clause (c) shall be omitted.

48. Omission of sections 91, 92, 93 and 94 : Sections 91,92,93 and 94 of the principal Act shall be omitted

49. Substitution of new Schedules for First Schedule and Second Schedule : For the First Schedule and the Second Schedule to the principal Act, the following Schedules shall be substituted, namely:—

"FIRST SCHEDULE

[See sub-section (4) of section 1]

DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY

Sl. No.	Description of documents or transactions
1.	A negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881 (26 of 1881)
2.	A power-of-attorney as defined in section IA of the Powers-of-Attorney Act, 1882. (7 of 1882)
3.	A trust as defined in section 3 of the Indian Trusts Act, 1882. (2 of 1882)
4.	A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 (39 of 1925) including any other testamentary disposition by whatever name called.
5.	Any contract for the sale or conveyance of immovable property or any interest in such property.

THE SECOND SCHEDULE

[See sub-section (1) of section 3A]

ELECTRONIC SIGNATURE OR ELECTRONIC AUTHENTICATION TECHNIQUE AND PROCEDURE

Sl. No.	Description	Procedure
(1)	(2)	(3)

50. Omission of Third Schedule and Fourth Schedule : The Third Schedule and the Fourth Schedule to the principal Act shall be omitted.

PART III

AMENDMENT OF THE INDIAN PENAL CODE

51.Amendment of Indian Penal Code : In the Indian Penal Code- (45 of 1860)

(a) Amendment of section 4 : in Section 4,-

(i) after clause (2), the following clause shall be inserted namely;

"(3) any person in any place without and beyond India committing offence targeting a computer resource located in India."

(ii) for the Explanation, the following Explanation shall he substituted, namely:-

'Explanation. - In this section—

(a) the word "offence" includes every act committed outside India which, if committed in India, would be punishable under this Code;

(b) the expression "computer resource" shall have the meaning assigned to it in clause (k) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000).';

(b) in section 40, in clause (2), after the figure "117" the figures and word "118, 119 and 120" shall be inserted;

(c) in section 118, for the words “voluntarily conceals, by any act or illegal omission, the existence of a design”, the words “voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design" shall be substituted;

(d) in section 119, for the words "voluntarily conceals, by any act or illegal omission, the existence of a design”, the words “voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design” shall be substituted;

(e) in section 464, for the words “digital signature” wherever they occur, the words “electronic signature” shall be substituted;

PART IV

AMENDMENT OF THE INDIAN EVIDENCE ACT, 1872

52. Amendment of Indian Evidence Act : In the Indian Evidence Act, 1872 (1 of 1872),—

(a) Amendment of section 3 : (a) in section 3 relating to interpretation clause, in the paragraph appearing at the end, for the words “digital signature” and “Digital Signature Certificate”, the words “electronic signature” and "Electronic Signature Certificate" shall respectively be substituted;

(b) Insertion of new section 45A:- after section 45, the following section shall be inserted, namey:-

"45A. Opinion of Examiner of Electronic Evidence.- When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000 (21 of 2000), is a relevant fact.

Explanation.- For the purposes of this section, an Examiner of Electronic Evidence Shall be an expert”

(c) Amendment of section 47A : In section 47A,

(i) for the words “digital signature”, the words “electronic signature” shall be substituted

(ii) for the words “Digital Signature Certificate”, the words “Electronic Signature Certificate” shall be substituted;

(d) Amendment of section 67A : in section 67A, for the words “digital signature” wherever they occur, the words “electronic signature" shall be substituted;

(e) Amendment of section 85A : in section 85A, for the words “digital signature” at both the places where they occur, the words “electronic signature” shall be substituted;

(f) Amendment of section 85B : in section 85B, for the words “digital signature" wherever they occur, the words “electronic signature" shall be substituted;

(g) Amendment of section 85C : in section 85C, for the words "Digital Signature Certificate” the words ‘‘Electronic Signature Certificate” shall be substituted.

(h) in section 90A for the words "digital signature" at both the places where they occur, the words “electronic signature” shall be substituted;

T.K. VISWANATHAN
Secy. to the Govt. of India

CORRIGENDUM

to

THE INDIAN BOILERS (AMENDMENT) ACT, 2007

(No. 49 of 2007)

In the Indian Boilers (Amendment) Act, 2007 (No. 49 of 2007), as published in the Gazette of India, Extraordinary, Part II, Section I, dated the December 13, 2007 (Issue No. 56),-

At page 6, line 17, for "(6)", read "(5A)".

ಕರ್ನಾಟಕ ರಾಜ್ಯಪಾಲರ ಆದೇಶಾನುಸಾರ ಮತ್ತು ಅವರ ಹೆಸರಿನಲ್ಲಿ,

ಆರ್. ಆಂಜಿನಿ

ಸಹಾಯಕ ಪ್ರಾರೂಪಕಾರ ಮತ್ತು ಪದನಿಮಿತ್ತ
ಸರ್ಕಾರದ ಅಧೀನ ಕಾರ್ಯದರ್ಶಿ,
ಸಂಸದೀಯ ವ್ಯವಹಾರಗಳು ಮತ್ತು ಶಾಸನ ರಚನೆ ಇಲಾಖೆ.

ಪಿ.ಆರ್. 27